UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/746,015	12/26/2000	Glenn Langford	77666-8/jpw	2269

7380 7590 08/31/2007

SMART & BIGGAR
P.O. BOX 2999, STATION D
900-55 METCALFE STREET
OTTAWA, ON K1P5Y6
CANADA

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
08/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/746,015
Filing Date: December 26, 2000
Appellant(s): LANGFORD, GLENN

Christine Genge
Reg. No. 45,405
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed May 18, 2007 appealing from the Office action mailed March 17, 2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 13-30 and 38-42 are rejected under 35 U.S.C. 102(b).

Claims 1 – 12 and 31 – 37 are rejected under 35 U.S.C. 103(a).

Claims 13-30 and 38-42 are rejected under 35 U.S.C. 102(b) as being anticipated by Ford et al. (U.S. Patent 5,481,613).

Regarding claim 13, Ford discloses:

A key release method comprising:

receiving a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext from a decryptor (Figure 2, column 6 lines 24 – 40);

locating decryptor authorization logic stored externally to the decryptor with use of the key related information (Figure 2, column 6 lines 50-55);

obtaining decryptor information in respect of the decryptor (column 6 lines 42 – 65); and

deciding based on the decryptor information and the decryptor authorization logic whether decryption of the key ciphertext is to be permitted (column 6 lines 56 – 66).

Regarding claim 29, Ford discloses:

A method of controlling access to a decryption key comprising:

receiving from a decryptor a key release request comprising decryptor information and the decryption key encrypted using a public key (Figure 2 step 34, column 6 line 40 – column 7 line 49);

locating decryptor authorization logic stored externally to the decryptor with use of the key related information (Figure 2, column 6 lines 50-55);

applying the decryption authorization logic to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key (column 7 lines 35 – 49);

upon determining the decryptor should be permitted access to the decryption key, sending a key release response specifying the decryption key (column 7 lines 35 – 49).

Regarding claim 30, Ford discloses:

A method of controlling access to decryption keys comprising:

maintaining a private key repository comprising a plurality of access identifiers, and for each access identifier at least one key related information of a respective {public key, private key} pair, the repository also containing the private key of each {public key, private key} pair (column 5 line 26 – column 6 line 33);

receiving a key release request containing a decryption key encrypted using a public key of a {public key, private key} pair and containing a key related information associated with the (public key, private key} pair (column 7 lines 35 – 49);

maintaining a repository residing externally to the key release request associating each access identifier with respective decryptor authorization logic that can be applied to a decryptor information (Figure 6, lines 50-55);

obtaining decryptor information (Figure 2 step 34, column 6 line 40 – column 7 line 49, Figure 6, lines 50-55)

for each access identifier in association with which the key related information is stored, applying the respective decryptor authorization logic to the decryptor information specified in the key release request (column 7 lines 35 – 49);

in the event the decryptor information satisfies at least one of the respective decryptor authorization logics, decrypting the ciphertext to recover the decryption key, and sending a key release response to the decryptor specifying the decryption key (column 7 lines 35 – 49).

Regarding claim 38, Ford discloses:

A key release agent comprising:

means for receiving from a decryptor a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext (Figure 2 step 34, column 6 line 40 – column 7 line 49);

means for locating decryptor authorization logic stored externally to the decryptor with use of the key related information (Figure 6, lines 50-55);

means for obtaining decryptor information in respect of the decryptor (Figure 2 step 34, column 6 line 40 – column 7 line 49, Figure 6, lines 50-55);

means for deciding based on decryptor information of the decryptor and the decryptor authorization logic whether decryption of the key ciphertext is to be permitted (column 7 lines 35 – 49).

Claim 14 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein the decryptor information is received from the decryptor together with the key ciphertext and key related information (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 15 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein obtaining decryptor information comprises receiving the decryptor information while establishing a secure connection with the decryptor (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 16 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein obtaining decryptor information comprises:

receiving from the decryptor a decryptor identifier (Figure 2 step 34, column 6 line 40 – column 7 line 49);

using the decryptor identifier to lookup decryptor attributes from a public repository, the decryptor identifier and decryptor attributes together constituting the decryptor information (Figure 2, column 6 line 42 – 65).

Claim 17 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

using information in a certificate as the decryptor information (column 6 lines 42 – 55).

Claim 20 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein the decryptor information is an identity or role of the decryptor, an alias, or a claim of access rights or privilege, or some other attribute of the decryptor of a corresponding decrypting device or platform (column 6 line 40 – column 7 line 49).

Claim 21 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein the key related information comprises a key pair identifier (column 5 line 18 – column 6 line 32).

Claim 22 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

decrypting the key ciphertext, re-encrypting the key using a public key of a {public key, private key} pair to produce a re-encrypted key, the private key of which is available to the decryptor, and sending the re-encrypted key to the decryptor (column 7 lines 8 – 49).

Claim 23 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

decrypting the key ciphertext to obtain a decryption key (Figure 4, column 7 lines 35 – 50);

sending the decryption key to the decryptor over a secure channel (Figure 4, column 7 lines 35 – 50).

Claim 24 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

decrypting the key ciphertext to obtain a decryption key (Figure 4, column 7 lines 35 – 50);

using a symmetric key available to the decryptor, encrypting the decryption key with the symmetric key to produce an encrypted decryption key, and sending the encrypted decryption key to the decryptor (Figure 4, column 7 lines 35 – 50).

Claim 25 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 further comprising:

receiving a plurality of key ciphertexts and respective key related information from the decryptor and determining whether at least one private key required to decrypt a respective at least one key ciphertext of the plurality of key ciphertexts is available (Figure 2, column 6 lines 24 – 40);

using the respective key related information to locate respective decryptor authorization logic stored externally to the decryptor (Figure 6, lines 50-55); and

upon determining such at least one private key is available, deciding based on the decryptor information and the respective decryptor authorization logic whether decryption of at least one of the plurality of key ciphertexts is to be permitted (column 7 lines 35 – 49).

Claim 28 is rejected as applied above in rejecting claim 13. Furthermore, Ford discloses:

A method according to claim 13 wherein deciding based on decryptor information of the decryptor and the decryptor authorization logic whether decryption of the key

ciphertext is to be permitted comprises applying at least one rule of the decryptor authorization logic associated with the public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key (column 7 lines 35 – 49).

Claim 39 is rejected as applied above in rejecting claim 38. Furthermore, Ford discloses:

A key release agent according to claim 38 adapted to receive the decryptor information together with the key ciphertext and key related information (Figure 2, column 6 lines 24 – 40).

Claim 40 is rejected as applied above in rejecting claim 39. Furthermore, Ford discloses:

A key release agent according to claim 38 adapted to use a decryptor identifier to lookup decryptor attributes from a repository, the decryptor identifier and decryptor attributes together constituting the decryptor information (Figure 2, column 6 line 42 – 65).

Claim 41 is rejected as applied above in rejecting claim 38. Furthermore, Ford discloses:

A key release agent according to claim 38 further comprising:

decrypting means for decrypting the key ciphertext (column 7 lines 8 – 49).

encryption means for re-encrypting the key using a public key of a {public key, private key pair to produce a re-encrypted key, the private key of which is available to the decryptor (column 7 lines 8 – 49);

means for sending the re-encrypted key to the decryptor (column 7 lines 8 – 49).

Claim 42 is rejected as applied above in rejecting claim 38. Furthermore, Ford discloses:

A key release agent according to claim 38 further comprising:

means for applying decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information for determining whether the decryptor should be permitted access to the decryption key (column 7 lines 35 – 49).

Claim 18 is rejected as applied above in rejecting claim 17. Furthermore, Ford discloses:

A method according to claim 17 further comprising:

obtaining the certificate from a certificate repository (column 6 lines 42 – 55).

Claim 19 is rejected as applied above in rejecting claim 17. Furthermore, Ford discloses:

A method according to claim 17 further comprising receiving the certificate together with the key ciphertext and key related information (column 6 lines 42 – 55).

Claim 26 is rejected as applied above in rejecting claim 25. Furthermore, Ford discloses:

A method according to claim 25 further comprising:

decrypting one of the key ciphertexts using a corresponding private key to recover a decryption key (Figure 2, column 6 lines 24 – 40).

Claim 27 is rejected as applied above in rejecting claim 25. Furthermore, Ford discloses:

A method according to claim 25 wherein deciding based on decryptor information of the decryptor and the respective decryptor authorization logic whether decryption of at least one of the key ciphertexts is to be permitted comprises applying the respective decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information to determine whether the decryptor should be permitted access to the decryption key (column 7 lines 35 – 49).

Claims 1 – 12 and 31 – 37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ford et al. (U.S. Patent 5,481,613).

Regarding claim 1, Ford discloses:

A method for a decryptor to obtain a decryption key from a key release agent comprising:

a decryptor obtaining an encryption block comprising a data ciphertext requiring a decryption key to decrypt, the encryption block further comprising key related information associated with a first (public key, private key) pair, the encryption block further comprising a key ciphertext consisting of the decryption key encrypted by the first public key of the first {public key, private key) pair (Figure 2 step 34, column 6 line 40 – column 7 line 49);

the decryptor generating a key release request containing the key ciphertext, and the key related information and outputting the key release request to the key release agent, the key release request for use by the key release agent to locate decryptor authorization logic stored externally to the key release that is to be applied in determining whether or not to release the decryption key (Figure 2 step 34, column 6 line 40 – column 7 line 49, Figure 6, lines 50-55)

the decryptor receiving a key release response specifying the decryption key (column 7 lines 35 – 49).

Ford however discloses that the encryption block includes an access controlled decryption block (ACD). However, the use of the ACD is not necessary to the operation of the key release agent releasing the decryption key to a decryptor. The ACD is just another section of data, which cannot be altered without the use of a key release agent (KRA). The exclusion of the ACD does not prohibit the cited prior art from providing a decryptor obtaining an encryption block with key related information, the decryptor generating a key release request, or the decryptor receiving a key release response

specifying the decryption key which the claims delineate. Therefore it would have been obvious to one of ordinary skill in the art to exclude the use of the specific data structure designated as the ACD, and replace it with another data structure that just provides key related information and not the additional information associated with the ACD.

Regarding claim 31, Ford discloses a private key repository with key related information and associated private keys of a {public key, private key} pair and a decryptor authorization logic definition function adapted to allow the definition of decryptor authorization logic to be applied to decryptor information to determine eligibility to decrypt, and for each decryptor authorization logic to select one or more of the key related information in respect of which the rule is to be applied (column 7 lines 35 – 49). Ford does not explicitly disclose an administrative interface comprising a private key maintenance function adapted to allow adding and deleting of a key related information and associated private key of a {public key, private key} pair. However, Ford discloses that the private key and key related information are stored in databases and/or in a trusted server system (column 5 lines 22 – 35). Servers by nature have an administrative interface to manage data, which the keys and key related information are classified. Therefore the function of adding and deleting data (private key and key related information) is a normal function of a server system. Therefore it would have been obvious to one of ordinary skill in the art to incorporate the function of adding and deleting keys and key related data using the server system to achieve the benefits of increased security of the keys and keeping more recent keys. Also, if one key is

corrupted or discovered by a third party, it is obvious that the compromised key must be deleted and another must be added in its place. Therefore though not mentioned explicitly in the prior art, the function claimed is deemed obvious in view of the above arguments.

Regarding claim 33, Ford discloses:

A decryptor comprising:

means for obtaining an encryption block comprising a data ciphertext requiring a decryption key to decrypt, the encryption block further comprising key related information associated with a first {public key, private key pair, the encryption block further comprising a key ciphertext consisting of the decryption key encrypted by the first public key of the first (public key, private key) pair (Figure 2 step 34, column 6 line 40 – column 7 line 49);

means for generating a key .release request containing the key ciphertext, and the key related information and outputting the key release request to the key release agent (Figure 2 step 34, column 6 line 40 – column 7 line 49);

means for making decryptor information available to the key release agent, the decryptor information for use by the key release agent to obtain decryptor authorization logic stored externally to the key release request that is to be applied in determining whether or not to release the decryption key (Figure 6, lines 50-55);

means for receiving a key release response specifying the decryption key (column 7 lines 35 – 49).

Ford however discloses that the encryption block includes an access controlled decryption block (ACD). However, the use of the ACD is not necessary to the operation of the key release agent releasing the decryption key to a decryptor. The ACD is just another section of data, which cannot be altered without the use of a key release agent (KRA). The exclusion of the ACD does not prohibit the cited prior art from providing a decryptor obtaining an encryption block with key related information, the decryptor generating a key release request, or the decryptor receiving a key release response specifying the decryption key which the claims delineate. Therefore it would have been obvious to one of ordinary skill in the art to exclude the use of the specific data structure designated as the ACD, and replace it with another data structure that just provides key related information and not the additional information associated with the ACD.

Claim 2 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising the decryptor making the decryptor information available to the key release agent in determining decryptor attributes, the decryptor attributes for further use in determining whether or not to release the decryption key (column 6 lines 42-65).

Claim 3 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising the decryptor using the decryption key to decrypt the data ciphertext (Figure 4, column 7 lines 35 – 50).

Claim 6 is rejected as applied above in rejecting claim 2. Furthermore, Ford discloses:

A method according to claim 1 wherein the decryptor making the decryptor information available to the key release agent comprises providing a decryptor identifier which may be used to look up decryptor attributes stored in a repository external to the key release request (Figure 2 step 34, column 6 line 40 – column 7 line 49, Figure 6, lines 50-55).

Claim 7 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 wherein the key related information comprises a key pair identifier (column 7 lines 35 – 49).

Claim 8 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising:

before generating the key release request, the decryptor determining if the private key of the first {public key, private key} pair is available at the decryptor (column 6 lines 33 – 65);

upon determining the private key of the first {public key, private key} pair is not available at the decryptor generating the key release request (column 6 lines 33 – 65).

Claim 9 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 further comprising:

decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key, private key} pair to recover the decryption key (Figure 4, column 7 lines 35 – 50).

Claim 10 is rejected as applied above in rejecting claim 1. Furthermore, Ford discloses:

A method according to claim 1 wherein the encryption block comprises a plurality of key related information associated with a respective plurality of first {public key, private key} pairs, and a respective plurality of key ciphertexts each consisting of the decryption key encrypted by the public key of a respective one of the plurality of first {public key, private key} pairs associated with the plurality of key related information, the method comprising:

generating the key release request containing the plurality of key ciphertexts, and the associated plurality of key related information (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 32 is rejected as applied above in rejecting claim 31. Furthermore, Ford discloses:

An administrative interface according to claim 31 wherein the private key repository maintenance function is further adapted to store the key related information and associated private key of a public key, private key} pair in association with one of a plurality of access identifiers (column 5 line 26 – column 6 line 33); and

wherein the decryptor authorization logic definition function is further adapted to store each authorization logic in association with one of the plurality of access identifiers (column 7 lines 35 – 49).

Claim 35 is rejected as applied above in rejecting claim 33. Furthermore, Ford discloses:

A decryptor according to claim 33 further comprising means for using the decryption key to decrypt the data ciphertext (Figure 4, column 7 lines 35 – 50).

Claim 36 is rejected as applied above in rejecting claim 33. Furthermore, Ford discloses:

A decryptor according to claim 33 adapted to make the decryptor information available to the key release agent by including the decryptor information in the key release request (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 37 is rejected as applied above in rejecting claim 33. Furthermore, Ford discloses:

A decryptor according to claim 33 further comprising means for decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key, private key} pair to recover the decryption key (Figure 4, column 7 lines 35 – 50).

Claim 4 is rejected as applied above in rejecting claim 2. Furthermore, Ford discloses:

A method according to claim 2 wherein the decryptor making the decryptor information available to the key release agent comprises including the decryptor information in the key release request (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 5 is rejected as applied above in rejecting claim 2. Furthermore, Ford discloses:

A method according to claim 2 wherein the decryptor making the decryptor information available to the key release agent comprises the decryptor providing the decryptor information to the key release agent while establishing a secure connection with the key release agent (Figure 2 step 34, column 6 line 40 – column 7 line 49).

Claim 11 is rejected as applied above in rejecting claim 10. Furthermore, Ford discloses:

A method according to claim 10 further comprising:

before generating the key release request, determining if at least one private key of the plurality of first {public key, private key} pairs is available at the decryptor (column 6 lines 33 – 65);

upon determining none of the private keys of the plurality of first {public key, private key} pairs is available at the decryptor generating the key release request (column 6 lines 33 – 65).

(10) Response to Argument

The Appellant has argued:

That Ford does not teach that there is both decryptor authorization logic and decryptor information. The Appellate argues that the rejection teaches that the decryptor authorization logic and the decryptor information as having the same meaning, and that this interpretation is in error.

The Examiner contends that this interpretation is not in error, as the claim (claim 13) does not require the decryptor authorization logic and the decryptor information to be separate, but just that they are obtained and used in making a decision of whether to allow decryption. For this purpose, Ford teaches that a Key Release Agent (KRA), the agent in charge of the decryption decision, receives decryptor privilege attributes (decryptor information and decryptor authorization logic) and uses this information to determined if the decryptor is authorized, before it authorizes decryption (column 6, lines 58-67).

The Appellant further argues:

That the decryptor privilege attribute information is not "decryptor logic" as claimed, and therefore, that Ford fails to teach "locating decryptor authorization logic stored externally to the decryptor."

The Examiner contends that Ford does teach "locating decryptor authorization logic stored externally to the decryptor." The Examiner would like to point out that the "decryptor authorization logic" is stored and transmitted, as per the claims. This feature

qualifies the "decryptor authorization logic" as information used to make a decision on whether or not to release a decryption key. Ford teaches such information used to make a decision on releasing a decryption key. Ford teaches that the KRA will obtain decryptor privilege attribute information to verify that the requesting decryptor is authorized (column 6, lines 42-44), and that this information may be obtained by the decryptor or from a supporting (external) database (column 6, lines 53-56). This decryptor privilege information is used to make a decision (allow or disallow) on releasing the decryption key (Figure 2, step 38). This information used to make a decision is authorization logic as it is used to make a decision. Therefore, it is respectfully asserted that Ford does teach "locating decryptor authorization logic stored externally to the decryptor."

The Appellant further argues:

That Ford does not teach obtaining the decryptor information from the decryptor nor receiving it together with the key ciphertext and key related information.

The Examiner contends that Ford does teach obtaining decryptor information from the decryptor and that the information is sent with the key ciphertext and key related information. Ford states "the decryptor privilege attributes, which maybe supplied by the decryptor through the key release request or by the database" (column 6, lines 58-62). This passage explicitly mentions that the decryptor information is received from the decryptor, and that it can be received through the key release request. Ford then discloses that the key release request must be protected, such as

by encryption, and use integrity mechanisms, such as digitally signing the request (column 7, lines 1-8). This encrypted key release request is "key ciphertext" and key related information, is the key release request itself, as it is regarding the release of the key. Therefore, the examiner respectfully asserts that Ford does teach obtaining the decryptor information from the decryptor and receiving it with the key ciphertext and key related information.

The Appellant further argues:

That Ford does not teach "obtaining the decryptor information from the decryptor" and furthermore, that Ford does not teach "establishing a secure connection with the decryptor while obtaining the decryptor information."

The Examiner contends that Ford does teach both obtaining the decryptor information from the decryptor and establishing a secure connection with the decryptor while obtaining the decryptor information. Ford states "the decryptor privilege attributes, which maybe supplied by the decryptor through the key release request or by the database" (column 6, lines 58-62). This passage explicitly mentions that the decryptor information is received from the decryptor, and that it can be received through the key release request. Ford then discloses that the key release request must be protected, such as by encryption, and use integrity mechanisms, such as digitally signing the request (column 7, lines 1-8), which is a secure connection as it both encrypts and repudiates the transaction. Therefore, the Examiner respectfully asserts that Ford does

teach both obtaining the decryptor information from the decryptor and establishing a secure connection with the decryptor while obtaining the decryptor information.

The Appellant further argues:

That Ford does not teach using a decryptor identifier to lookup decryptor attributes.

The Examiner contends that Ford does teach using a decryptor identifier to lookup decryptor attributes. Ford teaches that he KRA, which makes the decision on whether to release the key to the decryptor, may received the decryptor's authenticated identity (identifier) (column 6, lines 42-48), and then from an external database, obtain decryptor privilege attributes (column 6, lines 53-55), which can only be done if the KRA knows for which decryptor (identifier) the attributes are being obtained for. Therefore, it is respectfully asserted that Ford teaches using a decryptor identifier to lookup decryptor attributes.

The Appellant further argues:

That Ford does not teach receiving the certificate together with the key ciphertext and key related information.

The Examiner contends that Ford does teach receiving the certificate together with the key ciphertext and key related information. Ford states "the decryptor privilege attributes, which maybe supplied by the decryptor through the key release request or by the database" (column 6, lines 58-62). Information sent with the key release request,

can include a certificate (column 6, lines 51-53), wherein the key request is encrypted and signed (column 7, lines 1-7). This encrypted key release request is "key ciphertext" and key related information, is the key release request itself, as it is regarding the release of the key. Therefore, the examiner respectfully asserts that Ford does teach receiving the certificate together with the key ciphertext and key related information.

The Appellant further argues:

That Ford does not teach using key related information to locate the logic or deciding based on the logic in combination with the decryptor information whether the decryption is permitted.

The Examiner contends that Ford teaches both using key related information to locate the logic and using the logic and the decryptor information to determine whether the decryption is permitted. Ford discloses that the key related information, such as a private key ID (column 6, lines 5-9), is received at the KRA, and then used, to retrieve decryptor privilege attributes from an external database (column 6, lines 52-55). Therefore, Ford teaches locating the logic based on the key related information. Furthermore, Ford teaches using the decryptor attribute information (decryption information) to determine if the decryptor is authorized to access the decryption key (column 6, lines 58-67).

The Appellant further argues:

That Ford does not teach locating decryptor authorization logic stored externally to the decryptor.

The Examiner contends that Ford does teach locating decryptor authorization logic stored externally to the decryptor. The Examiner would like to point out that the "decryptor authorization logic" is stored and transmitted, as per the claims. This feature qualifies the "decryptor authorization logic" as information used to make a decision on whether or not to release a decryption key. Ford teaches such information used to make a decision on releasing a decryption key. Ford teaches that the KRA will obtain decryptor privilege attribute information to verify that the requesting decryptor is authorized (column 6, lines 42-44), and that this information may be obtained by the decryptor or from a supporting (external) database (column 6, lines 53-56). This decryptor privilege information is used to make a decision (allow or disallow) on releasing the decryption key (Figure 2, step 38). This information used to make a decision is authorization logic as it is used to make a decision. Therefore, it is respectfully asserted that Ford does teach "locating decryptor authorization logic stored externally to the decryptor."

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

(12) Conclusion

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

KA 08/22/2007 KA. 8/23/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Conferees:

Gilberto Barron
SPE 2132

/Benjamin Lanier/
Benjamin Lanier
Patent Examiner
GAU 2132